Definition of Cybersecurity

Gaps and overlaps in standardisation

V1.0

DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This report has been written by an expert group formed by members of the ETSI/CEN/CENELEC Cybersecurity Coordination Group (CSCG) and ENISA. The main contributors include:

- Charles Brookson – Zeata Security Ltd
- Scott Cadzow
- Ralph Eckmaier
- Jörg Eschweiler
- Berthold Gerber
- Alessandro Guarino – UNI
- Kai Rannenberg – Goethe University Frankfurt, DIN
- Jon Shamah
- Sławomir Górniak – ENISA

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank the numerous experts from Standards Development Organisations, industry, foundations and others who reviewed this paper for their contributions.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN 978-92-9204-155-7 DOI 10.2824/4069

Table of Contents

Executive Summary

In response to the European Union's Cybersecurity Strategy[1], the CSCG[2] has published a White Paper[3] with recommendations on digital security as essential capability to digital souverainity and a digital society. The CSCG's recommendations underline the importance of Cybersecurity standardisation to complete the European internal market and to raise the level of Cybersecurity in Europe in general. CSCG Recommendation #2 proposes a review of the definitions of the term 'Cybersecurity'. This document analyses the usage of this term by various stakeholders and reviews standardisation activities in the area of Cybersecurity, providing an overview of overlaps and gaps in available standards. It has been written by CSCG and ENISA experts as a response to the Recommendation #2 and forms a logical entity together with the response to the CSCG Recommendation #1, *Governance framework of the European standardisation – Aligning Policy, Industry and Research*, published by ENISA at the same time. Both documents will be presented for approval at the next CSCG plenary that is scheduled to take place in Berlin, 14-15 January 2016. As a result of the discussion at the CSCG plenary meeting and feedback received revised versions of the documents might be produced.

In language terms 'Cybersecurity' or 'cyber security', depending on the organization and the spelling of the word within its context, is a rather young term. Originated on the term 'Cyber Space', the term 'Cybersecurity' was crafted and used by IT professionals, consultants, lobbyists and politics to address security concerns in the 'Cyber Space'. But what does this mean? Does 'Cybersecurity' only address risks originating in the 'Cyber Space'? Does 'Cyber security' only consider the protection of virtual assets within the 'Cyber Space'? Does 'Cyber security' also apply to physical assets, such as Industrial Control Systems, production lines, power plants, etc. although they are not primarily designed to be in the 'Cyberspace'?

The first purpose of this document is to raise and describe these diverging understandings in more detail and provide a guide for determining an appropriate understanding of the term 'Cybersecurity' to be used in the context of the intended use of the stakeholders and policy makers. ENISA on behalf of the CSCG puts forward definitions of this term as well as the argumentation supporting its proposals[4]. The geographic boundaries are intended to be within the European Union, the member states and the European Standardization Organizations (ESO).

The second goal of this document is to list organisations taking part in standardisation in the area of Cybersecurity, provide an overview of activities and identify gaps and overlaps. Within Europe the three European Standards Organizations, CEN, CENELEC, and ETSI cooperate to try and minimize the amount of duplication of standards. However, there are many hundreds of groups that work on security or have security related work streams, and working together between these groups has proved to be difficult. In many cases gaps in standardization are being addressed, but probably not at a sufficient level of

[1] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
[2] ETSI CEN CENELEC Cybersecurity Coordination Group, http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx
[3] Recommendations for a Strategy on European Cybersecurity Standardisation ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/DefenceSecurityPrivacy/Cybersecurity/CSCG_WhitePaper2014.pdf
[4] This document is a proposal developed in collaboration with members of the CSCG. It will be presented for approval at the next CSCG plenary that is scheduled to take place in Berlin, 14-15 January 2016. As a result of the discussion at the CSCG plenary meeting and feedback received revised versions of the report might be produced.

commonality in order to insure that enough thorough security exists for new products and services when they are being developed.

Is there a need for a definition? Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers. Therefore, a contextual definition, based on one that is relevant, fits, and is already used a particular SDO or organisation should be considered. This document provides recommendations for stakeholders and policymakers, for terminology and for SDOs.

Stakeholders and policymakers should consider the definitions as explained and choose the most appropriate SDO and definition when considering their requirements. By referencing a specific definition (and any exceptions to that definition in the requirements), clarity can be maintained.

Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace.

SDOs are encouraged to embrace the concept of cybersecurity as the provision of security capabilities to apply to cyberspace. Existing use of the terms under the CIA paradigm when applied to single interfaces and single classes of object shall explicitly not use the term Cybersecurity.

The best way to ensure that there are no overlaps in standardisation related to Cybersecurity would be for the SDOs to ensure availability of a catalogue of standardisation activities and to introduce a method of referring to Standards so that impacts of changes can easily be tracked in dependencies.

There are three strands to standards development – overall requirements for security, privacy, and other related requirements; overall business requirements, security risks and threats; and security tools and techniques. We recommend that efforts are made to bring together the various requirements and initiatives in strand one. More work is required to identify risks and threats in strand two. We should work on a rationalization of techniques that we are using in strand three towards a smoother integration of protection into existing and emerging services and infrastructures.

1. Introduction

In the Cybersecurity strategy of the European Union, the EU reaffirms the importance of all stakeholders in the current Internet governance model and supports the multi-stakeholder governance approach. Indeed, the multi-stakeholder approach is fundamental to the development of successful standards, particularly in the area of Cybersecurity where public sector requirements are implemented to a large extent by private sector service providers.

In the field of promoting a Single Market for Cybersecurity products, the Cybersecurity strategy underlines the importance of the ETSI CEN CENELEC Cybersecurity Coordination Group (CSCG) and ENISA, by stating: “the Commission will support the development of security standards”; “Such work should build on the on-going standardisation work of the European Standardisation Organisations (CEN, CENELEC and ETSI), of the Cybersecurity Coordination Group (CSCG) as well as on the expertise of ENISA, the Commission and other relevant players”.

The Cybersecurity Coordination Group (CSCG) of CEN, CENELEC and ETSI is the only joint group of the three officially recognised European Standardisation Organisations with a mandate to coordinate Cybersecurity standards within their organisations. The CSCG was created in late 2011 to provide strategic advice on standardisation in the field of IT security, Network and Information Security and Cybersecurity.

In response to the European Union’s Cybersecurity Strategy, the CSCG has published a White Paper with recommendations on digital security. The CSCG’s recommendations underline the importance of Cybersecurity standardisation to complete the European internal market and to raise the level of Cybersecurity in Europe in general.

CSCG Recommendation #2 states:

The EC should establish a clear and common understanding of the scope of Cyber Security, based on an initiative the CSCG plans to launch to clarify the key terms and definitions used in the standardisation of and communication related to Cyber Security within the European Union. To establish clear understanding, the CSCG recommends that the European Commission should harmonise its usage of the key terms “Cyber Security”, “NIS” and “cybercrime” across the EU on the basis of existing definitions. Official communications currently use all three terms without distinguishing between them, which risks them being interpreted differently in different EU Member States (or languages). The CSCG recommends that the European Commission should not limit its clarification to definitions but should also establish an agreed understanding of the interdependencies and relationships between the three areas in question. The CSCG also recommends that the Commission should establish and enforce a suitable governance model for the three areas, with special emphasis on avoiding working in silos on topics that are inherently intertwined.

The CSCG decided at the meeting in Cyprus, 9-10 September 2014 to concentrate on the term ‘Cybersecurity’.

In language terms ‘Cybersecurity’ or ‘cyber security’, depending on the organization and the spelling of the word within its context, is a rather young term. Originated on the term ‘Cyber Space’, the term ‘Cybersecurity’ was crafted and used by IT professionals, consultants, lobbyists and politics to address security concerns in the ‘Cyber Space’. But what does this mean? Does ‘Cybersecurity’ only address risks originating in the ‘Cyber Space’? Does ‘Cybersecurity’ only consider the protection of virtual assets within the ‘Cyber Space’? Does ‘Cybersecurity’ also apply to physical assets, such as Industrial Control Systems, production lines, power plants, etc. although they are not primarily designed to be in the ‘Cyberspace’.

Additional to this controversy, the term ‘Cybersecurity’ is understood by some people as a synonym for the terms ‘IT security’, ‘ICT security’ or ‘information security’.

Is the ‘Cyber’ in ‘Cybersecurity’ a reference to the origin of the threats or does it apply to the assets being part of the ‘Cyberspace’ or some combination?

Finding a common understanding is a major challenge and it might not be possible to harmonize the definition and usage of the term.

The purpose of this document is:

- to raise and describe these diverging notions in more detail and provide a guide to determine an appropriate understanding of the term ‘Cybersecurity’ to be used in the context of the intended use of the stakeholders and policy makers. ENISA on behalf of the CSCG will put forward definitions of this term as well as the argumentation supporting its proposals[5]. The geographic boundaries are intended to be within the European Union, its member states and the European Standardization Organizations (ESO).
- to list organisations taking part in standardisation in the area of Cybersecurity, providing an overview of activities and identifies gaps and overlaps. Within Europe the three European Standards Organizations, CEN, CENELEC, and ETSI cooperate to try and minimize the amount of duplication of standards. However, there are hundreds of groups that work on security or have security related work activities, and working together between these groups has proved to be difficult. In many cases gaps in standardization are being addressed, but probably not at a sufficient level of commonality in order to insure that enough thorough security exists for new products and services when they are being developed.

[5] This document is a proposal developed in collaboration with members of the CSCG. It will be presented for approval at the next CSCG plenary that is scheduled to take place in Berlin, 14-15 January 2016. As a result of the discussion at the CSCG plenary meeting and feedback received revised versions of the report might be produced.

2. Common understanding of Cybersecurity

The term cyber and its associated terms cyberspace (any spelling) and cybersecurity (any spelling) have drifted from the world of the arts and into the mainstream. For many years we have seen BBC's fictional Dr Who battle against the cybermen starting with their debut in 1966, we have William Gibson's introduction of the concept of cyberspace in his novel "Neuromancer" where he defines Cyberspace as *"… a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding"*, and we have dancers in the 1960s using the term to refer to a half improvised free dance. Even prior to the term cyber in these forms we see use of the term cybernetics developed by Norbert Wiener in his book "Cybernetics or Control and Communication in the Animal and the Machine" (MIT Press, 1948) where the term in used in reference to the control of complex systems in the animal world and in mechanical networks, in particular self-regulating control systems. This is a snapshot of the long cultural background through which the term has become commonplace, and inevitably multi-nuanced.

Preceding Gibson's use of the term cyberspace, the Control Data Corporation marketed a line of computers as "cyber" and in doing so fixed the term to computing and technology and moved the term further from its suggested Greek root of meaning "skilled in steering or governing", a root that Wiener's use of the term is much more closely aligned to. During the latter part of the 1980s and throughout the 1990s cyber was used as a prefix in many areas: Cybercrime (crime involving computers), cyberpunk (the genre of fiction that Gibson and others belong to), cybergoth (music fans who share characteristics of the goth movement with electronic music and decoration), cyberbullying (bullying using the internet and social media), cybersex (sex using the internet and electronically controlled tools), cyberwarfare (acts of war carried out across the internet against human and non-human targets) and so on. A plea was made to stop the use of cyber as a general purpose prefix but that appears to have fallen on deaf ears. The end result is that removing the prefix and accepting that today the internet and electronic communication and control are endemic really means that cyber-security has the same difficulty in finding a simple definition as security.

Even the correct spelling of 'Cybersecurity' is controversial and differing. Some publications use a single word 'Cybersecurity', others prefer a term consisting of two words 'Cyber Security'. To complicate things, even the capitalization is disputed – in many respects this mimics the issues surrounding the correct spelling and capitalisation of the term email (or e-mail, or E-mail, or E-Mail …).

In common parlance, 'Cybersecurity' is defined by The Oxford English Dictionary as "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". Following this interpretation, only the unauthorized and criminal misuse of information is covered. But the question remains, what about operational errors? Is the protection against a human error to provide essential services in the 'Cyberspace' not within the scope of 'Cybersecurity'? The term 'information security' on the contrary includes the protection against such non-malicious disruptions.

Looking further into the definition of The Oxford English Dictionary, the question comes up about the manipulation of physical assets, such as production lines, utilities, etc. Is this covered by this definition?

However in the Standards community, the definition is significantly wider to include protection against a variety of risks for organisations and data, especially when 'Cybersecurity' is considered a synonym for 'Information security'.

The issue is even further compounded by the popularisation of the term in the mass media. The mass media commonly use it as a catch-all and 'dumbed-down' phrase that often attributes anything and everything that can disrupt computers as threats to 'Cybersecurity'.

In the military environments, organizations approach the term 'Cybersecurity' from an even wider and much more strategic perspective, using the term 'Cybersecurity' in connection with the terms "cyber defence" and 'cyber war'.

Figure (1) illustrates the different domains within the term 'Cybersecurity'.

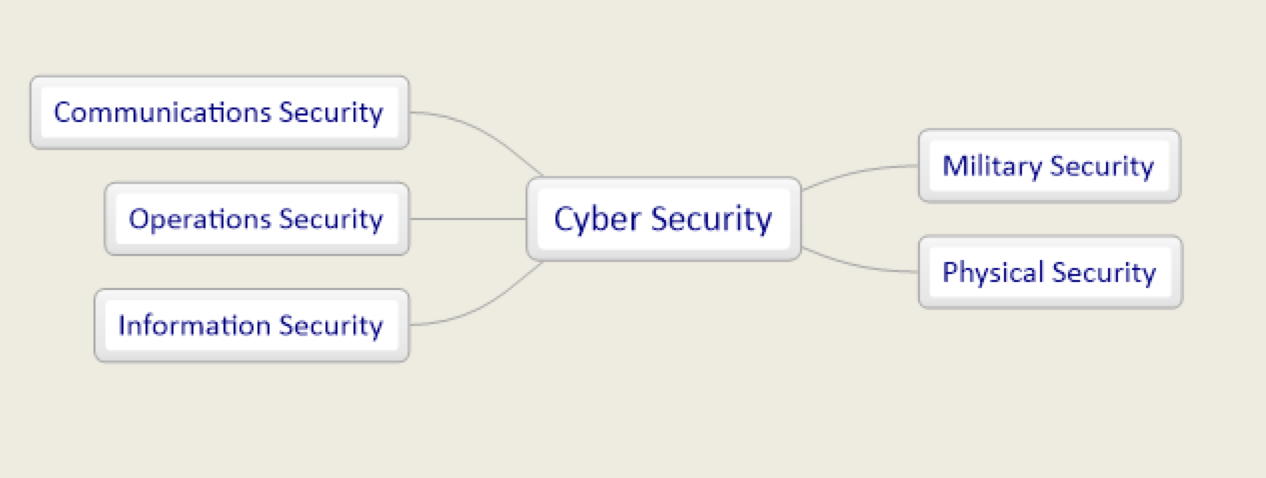

Figure 1: Different domains of Cybersecurity

In Figure 1, the domains are referred to as follows:

Communications Security	Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users.
Operations Security	Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users.
Information Security	Protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system.

Physical Security	Protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families.
Public/National Security	Protection against a threat whose origin is from within cyberspace, but may threaten either physical or cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications financial system or other critical public or industrial infrastructures.

This document specifically restricts its scope to Cybersecurity issues which are not specifically related to aspects of Public/National or Physical Security.

3. Terminology of Cybersecurity in documentation

3.1 Composition of the Term

A deconstruction of the components that make up the definition of the 'Cybersecurity' domain is illustrated below. This diagram looks at the various aspects of the definition which are referred to and implied when the definition is used by stakeholders.

This wide range of components adds to the wide variations in meaning of the term and has a potential to obscure the true scope of a particular Cybersecurity action or intention.

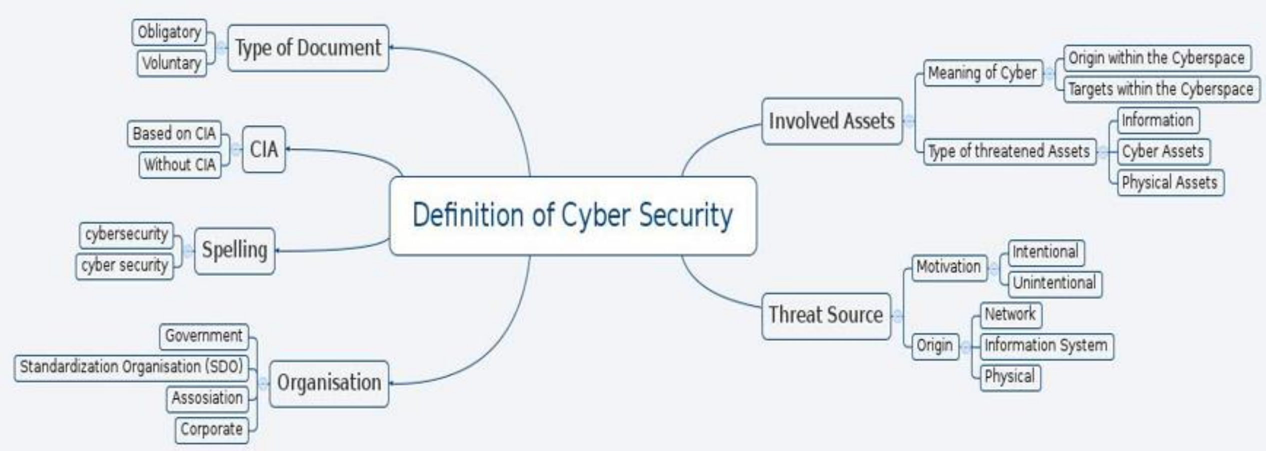

Figure 2: Components constituting the definition of Cybersecurity

The following is a detailed description of the origin of the definition described in figure 2.

Criteria	Explanation
Type of Document	Obligatory: A document that has a definition that is founded in law, regulations or mandatory standards.
	Voluntary: A document that has a definition that is founded in agreed best-practice or reputable recommendations
CIA	Based on CIA: The definition of 'Cybersecurity' uses and addresses the terms 'Confidentiality', 'Integrity' and 'Availability'
	Without CIA: The definition of 'Cybersecurity' does not refer to, or include the issues of 'Confidentiality', 'Integrity' and 'Availability'.
Spelling	The form of spelling that is being used. This provides consistency across a definition and its use.
Organization	The nature of the publishing organization may influence the factors or domains that are addressed in the definition. This may influence the stakeholder sectore applicability of the definition and therefore its usefulness.
Meaning of 'Cyber'	The definition refers to the origin of a threat that is introduced via Cyberspace rather than a physical attack.

	The definition looks only at targets that reduce the trustworthiness of a system or process rather than a device that is controlled via a system originating in the Cyberspace.
Types of threatened assets	Related to the above, the class of the threatened system that is covered in the definition of Cybersecurity'.
Motivation of Threat Source	The definition may address the motivation of the threat, whether by intent, for example criminal', or unintentional, as a result of a by-product of another action.
Origin of Threat Source	The definition may differentiate the origin of the threat. And may only consider protection against threats arising from the 'Cyber Space', aka Internet and are solely network based. Alternatively the definition may address the protection of Information Systems from local threats such as 'insider-threats'. Again, the definition may also address protection against physical attacks on the facility hosting Information Systems.

3.2 Terminology as defined by dictionaries

3.2.1 Oxford

The Oxford Dictionaries – Online[6] defines 'cybersecurity' as: *The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.*

3.2.2 Merriam Webster

The Merriam – Webster[7] defines 'cybersecurity' as: *Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*

3.3 Terminology used by organisations

The organisations mentioned below use the term 'Cybersecurity' in various contexts. They have been ordered according to their relevance for the European standardisation.

3.3.1 ETSI

Term	Cybersecurity
Organization	ETSI TC Cyber
Document Number	Not defined other than in the Terms of Reference of the ETSI Technical Committee CYBER
Document Title	Terms of Reference for ETSI TC Cyber
Publishing Date	n/a
Definition	n/a
Details	In ETSI TC CYBER has addressed Cybersecurity as domain with many facets and has identified both responsibilities and areas of activity to be undertaken across ETSI and in the technical body to address these. The main responsibilities of ETSI TC CYBER are: • To act as the ETSI centre of expertise in the area of Cybersecurity • Advise other ETSI TCs and ISGs with the development of Cybersecurity requirements

[6] http://www.oxforddictionaries.com/definition/english/cybersecurity?q=cyber+security

[7] http://www.merriam-webster.com/dictionary/cybersecurity

	• To develop and maintain the Standards, Specifications and other deliverables to support the development and implementation of Cybersecurity standardization within ETSI • To collect and specify Cybersecurity requirements from relevant stakeholders • To identify gaps where existing standards do not meet the requirements and provide specifications and standards to fill these gaps, without duplication of work in other ETSI committees and partnership projects • To ensure that appropriate Standards are developed within ETSI in order to meet these requirements • To perform identified work as sub-contracted from ETSI Projects and ETSI Partnership Projects • To coordinate work in ETSI with external groups such as Cybersecurity Coordination group in CEN CENELEC and ENISA • To answer to policy requests related to Cybersecurity, and security in broad sense in the ICT sector. These areas of responsibility are loosely mapped to “Areas of activity” that TC CYBER will address in close co-operation with relevant standards activities within and outside ETSI. The activities of ETSI TC CYBER include the following broad areas: • Cybersecurity • Security of infrastructures, devices, services and protocols • Security advice, guidance and operational security requirements to users, manufacturers and network and infrastructure operators • Security tools and techniques to ensure security • Creation of security specifications and alignment with work done in other TCs.
Reference	https://portal.etsi.org/TBSiteMap/CYBER/CyberToR.aspx

3.3.2 ISO/IEC JTC1

Both international SDOs decided in the past, that anything in the domain of Information Technology is neither solely ISO nor IEC but within both realms. Therefore they founded the Joint Technical Committee No.1 with the responsibility to develop standards within the domain of Information Technology.

Term	Cybersecurity
Organization	ISO/IEC JTC1/SC27 IT-Security Techniques
Document Number	ISO/IEC 27032:2012
Document Title	Information technology—Security techniques—Guidelines for cybersecurity
Publishing Date	2012
Definition	Preservation of confidentiality, integrity and availability of information in the Cyberspace
Details	Officially, ISO/IEC 27032 addresses “Cybersecurity” or “Cyberspace security”, defined as the “preservation of confidentiality, integrity and availability of information in the Cyberspace”. In turn “the Cyberspace” (complete with definite article) is defined as “the complex environment resulting from the interaction of people, software and

	services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.
Reference	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375

Additionally to the term ‘Cybersecurity’, ISO/IEC JTC1/SC27 developed definition for similar or equal terms worth being mentioned and considered.

Term	information security
Organization	ISO/IEC JTC1/SC27 IT-Security Techniques
Document Number	ISO/IEC 27000:2014
Document Title	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
Publishing Date	2014
Definition	Information security Preservation of *confidentiality*, *integrity* and *availability* of information Confidentiality Property that information is not made available or disclosed to unauthorized individuals, entities, or processes Integrity Property of accuracy and completeness Availability Property of being accessible and usable upon demand by an authorized entity
Details	The term ‘information security’ was previously contained as a definition in ISO/IEC 27002:2009 but due to the fact, that all definitions within the ISMS-family were transferred to ISO/IEC 27000, it was also relocated. All documents within the ISMS-family are to be seen as support for ‘ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements’, which is the main requirement standard of this family of standards. ISO/IEC 27001:2015 is a world-wide accepted Management System Standard for the implementation and maintenance of information security within an organization.
Reference	http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411 Freely available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

3.3.3 ITU

Term	cybersecurity
Organization	ITU-T
Document Number	X.1205
Document Title	SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Telecommunication security Overview of cybersecurity

Publishing Date	April 2008
Definition	cybersecurity The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
Details	Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.
Reference	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

High level terms used in ITU-T documents and their associated definitions can be found in Annex A.

3.3.4 NIST

Term	cybersecurity
Organization	NIST National Institute of Standards and Technology
Document Number	Special Publication 800-39
Document Title	Managing Information Security Risk Organization, Mission, and Information System View
Publishing Date	March 2011
Definition	cybersecurity The ability to protect or defend the use of cyberspace from cyber attacks.
Details	This definition is based on the definition of ‘cybersecurity’ contained in the 2010 version of NCSSI No.4009. The definition of ‘cybersecurity’ in No.4009 has been changed in the meantime (see chapter **Error! Reference source not found.**).
Reference	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

3.3.5 NATO

Term	Cyber security
Organization	NATO Cooperative Cyber Defence Centre of Excellence
Document Number	ISBN 978-9949-9211-2-6
Document Title	NATIONAL CYBER SECURITY FRAMEWORK MANUAL
Publishing Date	2012
Definition	No specific definition for ‘cyber security’ contained.
Details	“…In addition to the versatile threat landscape and the various players involved, the measures to address cyber threats come from a number of different areas. They can

	be political, technological, legal, economic, managerial or military in nature, or can involve other disciplines appropriate for the particular risks”
Reference	https://ccdcoe.org/sites/default/files/multimedia/pdf/NCSFM_0.pdf

3.3.6 CNSS

Term	cybersecurity
Organization	Committee on National Security Systems
Document Number	CNSSI No. 4009
Document Title	Committee on National Security Systems (CNSS) Glossary
Publishing Date	April 2015 / January 2008 (NSPD-54/HSPD-23)
Definition	cybersecurity Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Source: NSPD-54/HSPD-23 cybersecurity The ability to protect or defend the use of cyberspace from cyber attacks. Note 1: This definition was contained in the 2010 version of the CNSS Glossary. Note 2: This definition is still used In NIST SP800-39 (see chapter **Error! Reference source not found.**).
Details	This definition is taken over from the ‘Definitions’ contained in the National Security Presidential Directive (NSPD) -54/Homeland Security Directive (HSPD) -23 issued by President in January 2008.George W. Bush.
Reference	https://www.cnss.gov/CNSS/openDoc.cfm?yBg7QzXbL3NGs6wceKGXPw==

3.4 Summary of the usage of the Term Cybersecurity

The following table provides an overview of the identified definitions based on the criteria specified above:

Origin	Document	Spelling	Organization	Type	CIA	Meaning	Motivation	Threat
ISO/IEC JTC1/SC27	27032	Cybersecurity	SDO	V	YES	Only assets intended for the Internet	No differentiation between malicious or unintentional	Only virtual assets connected to the Internet, no physical assets
ISO/IEC JTC1/SC27	27000	Information security	SDO	O[8]	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
ITU-T	X.1205	cybersecurity	Inter-gov	???	YES	Any Risk origination in the Cyber Space	No differentiation between malicious or unintentional	Any asset
NIST	SP 800-39	cybersecurity	SDO	V	NO	Risk originating in the Cyber Space ONLY	Only covers malicious origins (cyber attacks)	Only virtual assets connected to the Internet, no physical assets
NATO	National Cyber Security Framework Manual	--	Military	V	NO	Any Risk origination in the Cyber Space (Cyber Threat)	Only covers malicious origins (cyber Threats)	Any asset
Committee on National Security Systems	CNSSI No. 4009	Cyber security	Govt	O	YES	Any Risk	No differentiation between malicious or unintentional	Any asset

[8] Because of its usage by ISO/IEC 27001.

4. Standardisation work in Cybersecurity

4.1 Organisations involved in standardisation

The following organisations are taking part in standardisation activities related to Cybersecurity – traditional SDOs and industrial associations.

Organisation	Type of organisation	Summary
3GPP – 3rd Generation Partnership Project	SDO partnership	3GPP unites six telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), and provides their members with a stable environment to produce the Reports and Specifications that define the world's principal mobile communication technologies. The scope includes cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, and quality of service. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks. http://www.3gpp.org/
CableLabs	Industry forum	CableLabs is the principle standards body globally for the providers and vendors in the cable industry. Its standards are republished by ETSI and ITU-T. http://www.cablelabs.com/
CEN – Comité Européen de Normalisation	European SDO	Provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes. Notably it is a member of the CSCG (Cybersecurity Coordination Group) to the EC. https://www.cen.eu/
CENELEC – European Committee for Electrotechnical Standardization	European SDO	CENELEC is responsible for standardization in the electrotechnical engineering field. Its Cybersecurity activity relates to coordination on smart grid information security. Notably it is a member of the CSCG (Cybersecurity Coordination Group) to the EC. http://www.cenelec.eu/
CSA – Cloud Security Alliance	Industry forum	CSA develops best practices for providing security assurance within Cloud Computing, and provides education on the uses of Cloud Computing to help secure all other forms of computing. https://cloudsecurityalliance.org/
ETSI – European Telecommunication Standards Institute	European SDO	ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged,

		broadcast and internet technologies. Notably, it hosts the Technical Committee for Cybersecurity and is a member of the CSCG (Cybersecurity Coordination Group) to the EC. < http://www.etsi.org/>
FIDO Alliance	Industry forum	The Fast IDentity Online organization develops technical specifications that define an open, scalable, interoperable set of mechanisms that reduce the reliance on passwords to authenticate users and promotes their use. https://fidoalliance.org/about/
GlobalPlatform	Industry forum	GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology. Its proven technical specifications, which focus on the secure element (SE), trusted execution environment (TEE) and system messaging. https://www.globalplatform.org/default.asp
GSMA – GSM Association	Industry forum	GSMA is the global *organization* of GSM and related mobile providers and vendors, and today the largest telecommunication industry entity. GSMA's Fraud and Security Working Group is the global mechanism for exchanging information, developing standards and techniques, and collaborating on mobile Cybersecurity in many other forums. It works closely with 3GPP groups, especially SA3 (Security) – providing support for Cybersecurity information assurance initiatives. http://www.gsma.com/
IEEE – Institute for Electrical and Electronic Engineers	Industry forum	The IEEE is the principal professional body of U.S. electrical and electronic engineers that maintains an array of publications, global standards activities and conferences – increasingly in the area of Cybersecurity. The IEEE Computer Society recently launched an initiative known as the Center for Secure Design with the aim of expanding and escalating its ongoing involvement in the field of cybersecurity. Its standards activities are principally in the area of SmartGrid and other critical infrastructure security. http://www.ieee.org/
IETF – Internet Engineering Task Force	Industry forum	The IETF is a global standards making activity of the Internet Society that influences the way people design, use, and manage the Internet. Many of these activities are Cybersecurity related. An entire Security Area includes. Its Internet

		Architecture Board (IAB) also oversees development of Cybersecurity capabilities. http://www.ietf.org
ISO – International Organization for Standardization	Global SDO	The ISO is a Swiss based private international standards development and publishing body composed of representatives from various national standards organizations with multiple committees – several of which have significant Cybersecurity related activity. http://www.iso.org
ITU – International Telecommunication Union	Global SDO	The ITU is a Swiss based intergovernmental body with three sectors dealing with the development and publication of Recommendations for radio systems (ITU-R), telecommunications (ITU-T), and development assistance (ITU-D). https://www.itu.int
OASIS – Organization for the Advancement of Structured Information Standards	Independent industry forum	OASIS is a major global industry body for developing and publishing worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas requiring structured information exchange. Although it began focussed on XML language schema, it has subsequently expanded to JSON. Its currently hosts the Cybersecurity technical committees listed below. https://www.oasis-open.org/org
OMG – Object Management Group	Industry forum	OMG is a computer industry consortium to develop enterprise integration standards. The Group's principal current Cybersecurity work deals with threat modelling where its System Assurance Task Force Security Fabric Working Group is developing a Unified Modeling Language Threat & Risk Model. http://sysa.omg.org/
TCG – Trusted Computing Group	Industry forum	TCG develops, defines and promotes open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. It platforms provide for authentication, cloud security, data protection, mobile security, and network access & identity. TCG presently has ten working groups. http://www.trustedcomputinggroup.org/
W3C – World Wide Web Consortium	Industry forum	W3C develops protocols and guidelines for WWW services. It maintains four Cybersecurity groups. http://www.w3c.org/

4.2 Areas covered by standardisation

Cybersecurity standardisation has been broken down into a number of areas dealing with different aspects of the security lifecycle of "Assess – Design – Manage – Monitor – Deploy" with many aspects of design, particularly in regard to standards addressing the traditional CIA paradigm. For the purposes of this consideration we look at standardisation aspects for the provision of security features (primitives, protocols, services), for the reporting of security threat information, and for the organisational management to give security assurance.

4.2.1 Security feature provision

Most technical standards bodies have prepared standards for the provision of sector/technology specific security features. As an example the 3G PLMN has a set of standards covering authentication of terminals, provision of air interface confidentiality (on the risk analysis result that the open air-interface is the interface that is the most at risk), provision of signalling and data integrity validation services, of key management for the cryptographic algorithms and the definition of the algorithms themselves including addressing the export control of them.

4.2.2 Security assurance

The security assurance field is dominated, in standards, by the Common Criteria initiative (ISO 15408) and by ongoing work in the 3GPP community. However in addition to this formal work a number of initiatives are led by industry with product quality testing by Apple for example covering product security, by Google for Android, and by Microsoft for the Windows platform.

It should be noted that it is not obligatory to adhere to any security assurance criteria and thus many products have unverified security capability.

4.2.3 Security threat sharing

Sharing of threat information, current attack patterns, software vulnerabilities and so forth has been standardised in process through the establishment of a network of CSIRTs (Computer Security Incident Response Teams) and been augmented by the establishment and development of a number of initiatives such as STIX/TAXII, CyBox, MISPs (Malware information Sharing Platform). Many of these initiatives are standardised with STIX/TAXII/CybOX recently moved to the OASIS standards track (and this will be closely followed by, amongst others, ETSI CYBER).

4.2.4 Organisational management for secure operations

The outstanding example in this domain is the ISO 27000 series of guides and recommendations. Within this series ISO/IEC 27001 is a certification standard that is designed to help an organization to define a framework for managing Information security more effectively which then points to ISO/IEC 17799 which lists controls and interpretation for the same. For more specific IT functions the COBIT guides add additional controls for implementing IT Governance within an organization, and ITIL extends these slightly in the domain of IT Service Management covered by ISO standards ISO 20000-1 (guidance) and ISO 20000-2 (certifiable standard).

Many individual nations have taken and either endorsed the ISO specifications as above or extended them (noting that the ISO specifications themselves have been derived from a large number of national and international security frameworks).

5. Overlaps in standardisation efforts

Standardisation activities take place in international, national, and industry-based forums. Within Europe the three European Standards Organizations, CEN, CENELEC, and ETSI cooperate to try and minimize the amount of duplication of standards. Many groups have liaisons and co-operation agreements within the various groups. However, there are many hundreds of groups that work on security or have security related work streams, and working together between these groups has proved to be difficult.

There are many examples of duplication of work between standards organizations: For example on the Internet of things we have work undertaken by ITU Study Group 20[9], oneM2M[10] and also specific work items in many other groups such as those looking at intelligent transport, Smart energy, Smart cities, and many other related activities.

Similar overlaps, including those that are security related occur in topics such as Mobile radio between 3GPP, some of the ITU work, and also work within IETF on protocols.

Over the years many papers and efforts have been produced highlighting works within standards organizations in order to highlight the overlaps. For example ITU has a Standards Roadmap[11] detailing different standards works, and some of the different and overlapping activities within organizations. The Roadmap was launched by ITU Study Group 17, and became a joint effort in January 2007, when the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG) joined the initiative, but it suffers from the immense effort needed to keep it current. A recent contribution to TC CYBER[12] has also highlighted standards in the Global Cybersecurity Ecosystem, and work going on worldwide in many areas.

Although this overlap is inevitable, organizations must ensure that they have sufficient contact between themselves to minimize the impact, as the number of experts in the security area capable of working on the subjects is necessarily limited.

When standards are being formulated, they should draw upon existing standards without change, or if any changes are required, they should be fed back into those existing standards. Theree is a serious impact if one standard draws directly from another standards, then changes in one standard are not reflected in others.

The best way to ensure lack of overlaps in Cybersecurity standardisation would be for the SDOs to:

- Ensure the availability of a Standards Catalogue, drawing upon the ITU, ENISA and NISSG initiative above.
- Introduce a method of referring to Standards so that impacts of changes can easily be tracked in dependencies.

[9] ITU-T SG20: IoT and its applications including smart cities and communities (SC&C) - http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx
[10] OneM2m Standards for M2M and the Internet of Things http://www.onem2m.org/
[11] ITU Standards Roadmap - http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/default.aspx
[12] Global Cybersecurity Ecosystem – ETSI TR 103 306 - https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?wki_id=45906

6. Gaps in standardisation activities

6.1 Overall situation

In some areas of standardisation, overlaps exists (like e.g. competing organizations as well as competing technical standardization approaches) and will probably persist due to the political interests of commercial as well as non-commercial organizations. Keeping in mind that monocultures usually lead to lower progress while competition usually fosters evolution, the fact of overlap itself might not be that much of an issue but mapping this to a limited amount of available resources (to e.g. participate in the process of standardization), a very dynamic market with limited ability as well as limited motivation to quickly adopt standards without "warranty" on sustainability could make the issue significant.

Some existing and well-accepted international standards (e.g. ISO/IEC 27035) are not reflected in European norms, so based on careful evaluation and counseling with relevant stakeholders an easy solution could be to adopt and reflect them into European norms where feasible. One should not focuson operational aspects only but drive the overall cybersecurity standardization approach on strategic level.

Looking at it from such a perspective, the first gap in standardization to approach would be the lack of a commonly accepted and formally standardized definition of the cyber domain. We also lack field-proven standards on how to timely and practically evaluate the quality and effectiveness of modern technologies that aim to provide protection against attacks.

Looking at the dynamically changing landscape of tools and technologies, the lack of applicable standards leads to the situation where technology vendors keep proprietary solutions, while consumers are left without transparency on their systems. Classic approaches to verification of technical requirements (e.g. Common Criteria Protection Profiles) are complex and hard to keep-up with in dynamic markets, technologies and changing threat landscape.

There are several globally acting large corporations based or originating in Europe, but the majority of the economic ecosystem is made of mid-sized and small companies. From the point of view of the type of business Europe has a globally strong position in Aerospace, Automotive, Chemicals, Defence, Engineering, High Tech, Pharmaceutics and related goods and services. Some of these are ran under national and international regulations and observe standards applicable to their fields. However, typical industry regulations do not cover Cybersecurity directly, but through rules on technical and ethical compliance and code of conduct of business.

Privacy is one of the core European basic rights. It is evident that especially this aspect seems to have been left-out in the technical standards. Some industry practice standards (e.g. PCI DSS) as well as specific requirements exist, but this is not sufficient to enable neutral evaluation of technologies nor services to the national or European privacy regulations.

It is observed that although the market demand is shifting from pure technology towards so-called Managed Security Services, there are yet no sustainable and accepted industry or conceptual standards available on this topic. Some national security authorities (like French ANSSI, German BSI and British CESG) started to work and pilot local schemes, partly overlapping but also following sometimes different approaches.

6.2 Mitigating the gaps

In many cases gaps in standardization are being addressed, but probably not at a sufficient level of commonality in order to ensure that new products and services benefit from an appropriate attention to security issues when they are being developed.

Areas in which there are many standards for example include:

- Identity and associated mechanisms such as frameworks and architectures (e.g. ISO/IEC 24760), identification and authorization protocols, (e.g. OpenID, OAuth, LID), Smart cards. However for areas like privacy-friendly authentication the more technical standards still don't exist.
- Confidentiality, with multiple algorithms and key distribution techniques,
- Integrity protection, some of which had to be modified when found to be insecure.
- Privacy and related mechanisms, which exist in many places, such as those from the GSMA and many other bodies: ISO/IEC JTC 1/SC 27, W3C, OECD and The Information Commissioner's Office in The United Kingdom.

It is probably true and that there will never be universal systems for the design of security into systems, products and services, and it can be argued that a diverse ecosystem of security techniques actually adds to the security protecting against surprising vulnerabilities of specific techniques. Nevertheless when new systems are being designed then it is vitally important that minimal changes, where possible, are made to existing protocols.

There is also overlap between standardisation activities such as the convergence between safety and security in critical infrastructure, the aeronautics industry and transport.

There are three strands to standards development, which we should consider:

- The first strand is setting the overall requirements for security, privacy, and other related security requirements. There are many examples of these from ISO/IEC JTC 1, NIST, and other similar frameworks. What is lacking is a coherent method for bringing together these various frameworks, so when a System, Service or Product has been developed, then the appropriate framework can be used. The number of these frameworks should be minimised or, at least, the relationships between them need to be better understood. There are also of course legal requirements, such as those for Data protection, law enforcement, and Business such as trading information, which may be sensitive. These requirements need also to be put into the framework.
- The second strand is concerned with looking at the overall business and identifying the security risks and threats. Too often security products and services are developed without understanding these important issues, and without considering the flexibility (such as replacing algorithms) and life cycle requirements from start to withdrawal from service.
- The third strand is that of security technical implementation, this is partly well covered by the various tools and techniques that exist. However there are many of these, and it would be useful to consider how these could be reduced to enable reuse when they are required. In this way they can more easily be built into Products and services and present a consistent Interface for the customer and operator. Also missing are standards and guidelines to integrate the tools and techniques towards systems, that can provide secure infrastructure services, e.g. as a basis for an infrastructure initiative to provide cryptographically protected end-to-end- encrypted communication to normal (non-expert) users. Also there is a lack of system standards for secure and trustworthy (device) platforms, that can function as terminals for end-to-end protection

usable by non-experts. Both are of importance if these services are to be made available in an affordable manner to ordinary citizens and small businesses, e.g. via universal service provision.

It is probably true to say that there are many different standards on several technologies available; what needs to be addressed is the reduction of the proliferation of very similar but incompatible tools and techniques and the provision of essential services to non-expert users.

We would recommend that efforts are made to bring together the various requirements and initiatives in strand one.

More work is required to identify risks and threats in strand two. We should work on a rationalization of techniques that we are using in strand three towards a smoother integration of protection into existing and emerging services and infrastructures.

One of the conclusions of the analysis of the existing approaches on standardization is that the landscape is very scattered, from e.g. process-related standards down to e.g. single technology standards without overall integration.

7. Recommendations

7.1 Is there a need for a definition?

There does not need to be a definition for Cybersecurity in the conventional sense that we tend to apply to definitions for simple things like authentication of an identity (a security mechanism allowing the verification of the provided identity). The problem is that Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers.

Therefore, a contextual definition, based on one that is relevant, fits, and is already used a particular SDO or organisation should be considered. Concrete examples of such usage have been provided in Section 3.3.

7.2 For stakeholders and policymakers

Stakeholders should have an easy to understand guide so that they may refer, unambiguously to the scope of Cybersecurity that they intend. Because of the breadth of the topic, as described, SDOs and other organizations all have differing definitions.

Stakeholders and policymakers should consider the definitions as explained and choose the most appropriate SDO and definition when considering their requirements. By referencing a specific definition (and any exceptions to that definition in the requirements), clarity can be maintained.

Based on the previous summary table in chapter 3.4, it is possible to use the following graphic representations as a guide to selection of the correct definition and associated spelling. In the following figures, fields marked in red represent the components of definitions used in specific context. The table (Figure 8) depicts comparison between the contexts.

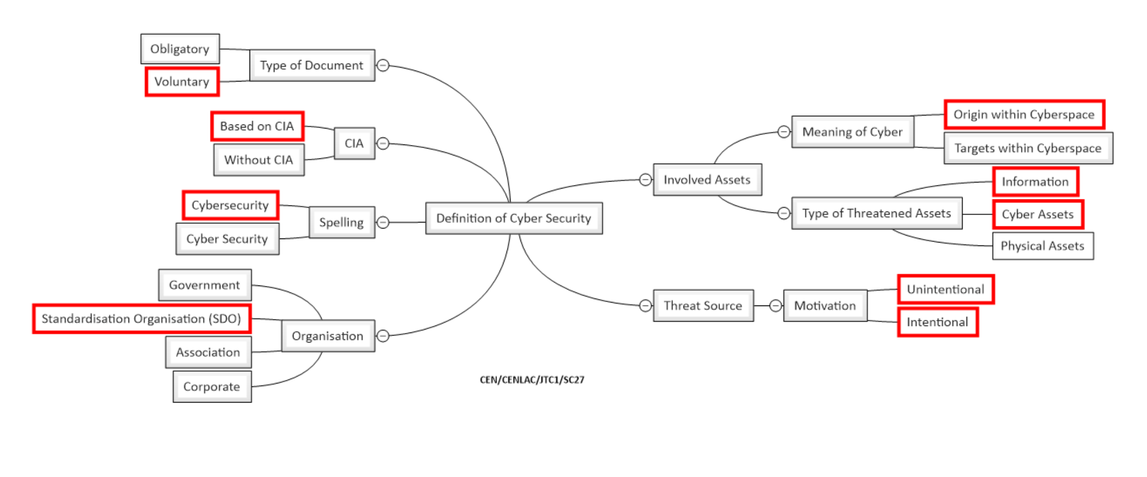

Figure 3: Inclusion of components by CEN/CENLAC/JTC1/SC27

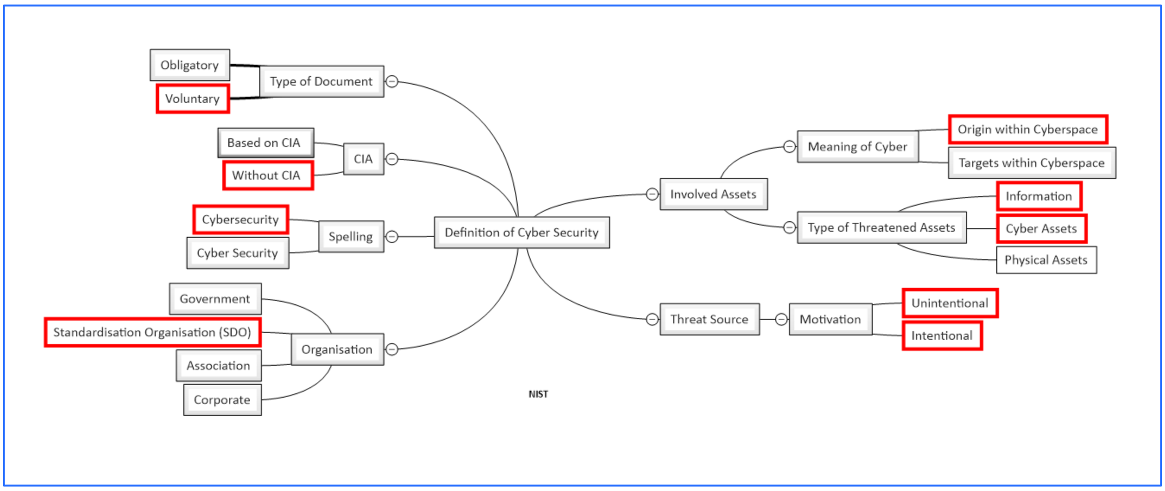

Figure 3: Inclusion of components by ITU-T

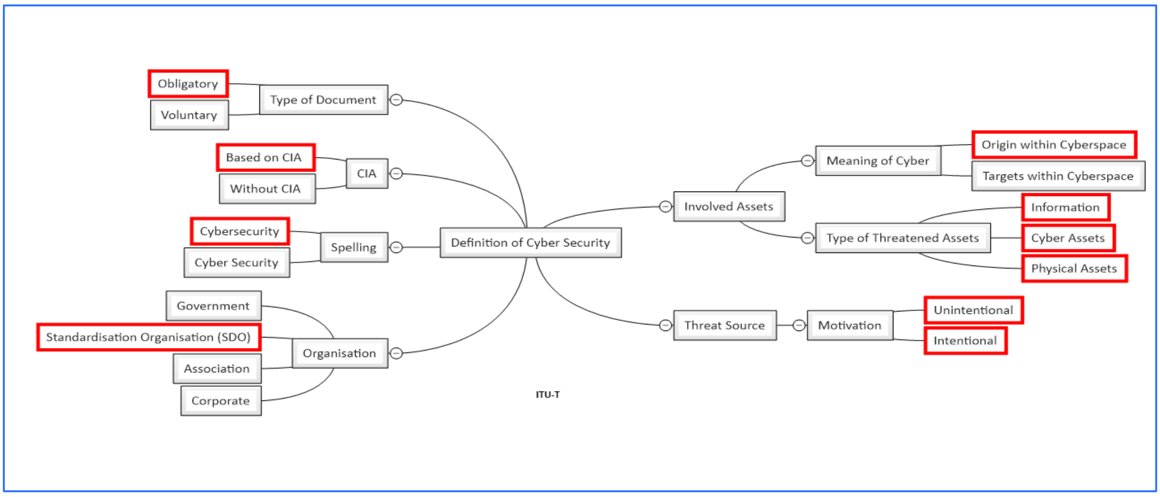

Figure 4: Inclusion of components by NIST

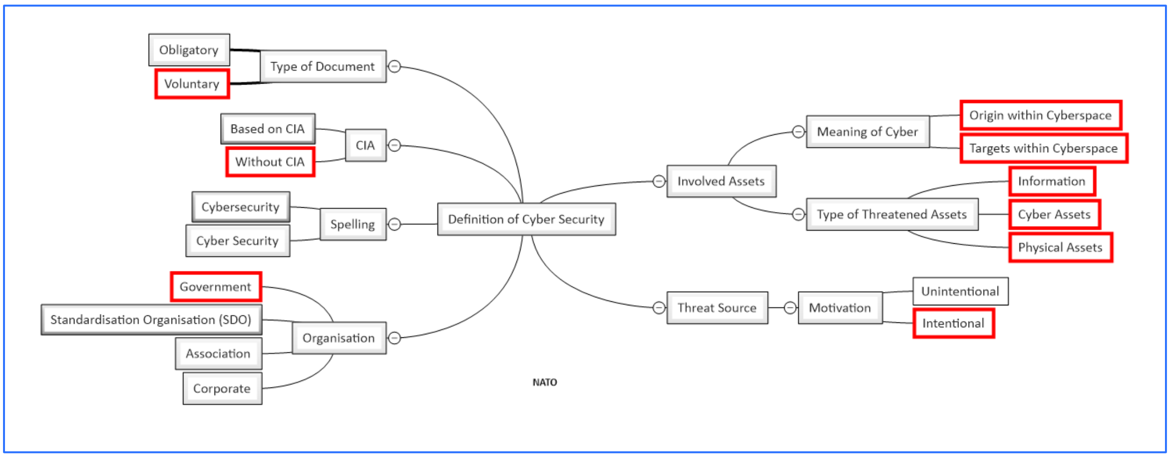

Figure 5: Inclusion of components by NATO

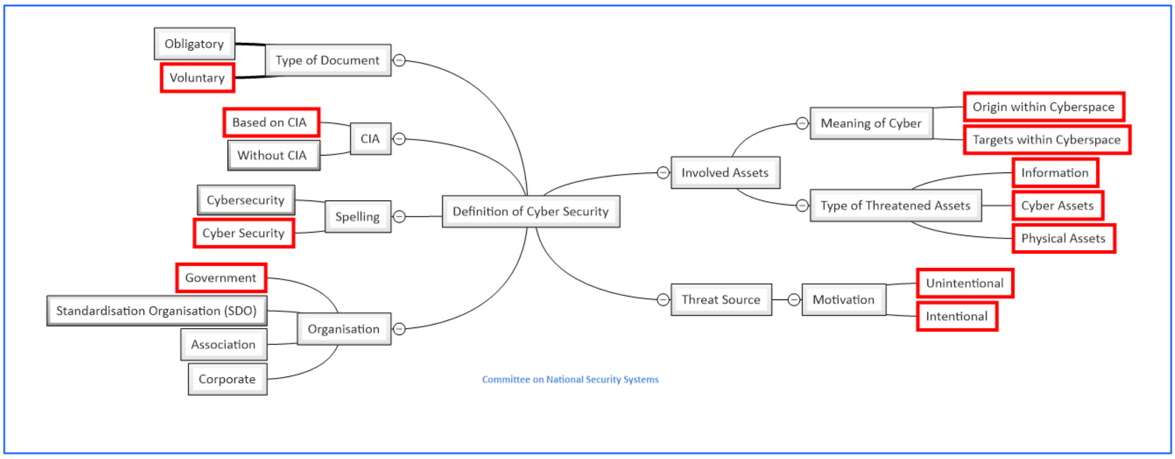

Figure 6: Inclusion of components by the Committee on National Security Systems

	Spelling	Type of Organisation	Type of Document		CIA		Involved Assets		Threatened Asssets			Motivation of source	
		SDO	Obligatory	Voluntary	Based on	Without	Origin in Cyberspace	Target in Cyberspace	Information	Cyber	Physical	Intentional	Unintentional
ISO/IEC JTC1/ SC27 27032	Cybersecurity	✓		✓	✓		✓		✓	✓		✓	✓
ISO/IEC JTC1/ SC27 27000	Information Security	✓	✓	□		✓	✓		✓	✓		✓	✓
ITU-T	Cybersecurity	✓	✓		✓		✓		✓	✓	✓	✓	✓
NIST	Cybersecurity	✓		✓		✓	✓		✓	✓		✓	✓
NATO				✓		✓	✓	✓	✓	✓	✓	✓	
CNSS	Cyber security			✓	✓		✓	✓	✓	✓	✓	✓	✓

Figure 8: Tabular comparison

7.3 For terminology

Cybersecurity shall refer to security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that Cyberspace. Cybersecurity shall therefore encompass the CIA paradigm for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack).

7.4 For SDOs

SDOs are encouraged to embrace the concept of cybersecurity as the provision of security capabilities to apply to cyberspace. Existing use of the terms under the CIA paradigm when applied to single interfaces and single classes of object shall explicitly not use the term Cybersecurity.

Annex A: Terminology used by ITU

The following are high level terms used in ITU-T documents and their associated definitions:

Document:	**ITU-T X.1205 (04/2008)**	
Term	Ref	Definition
access point (ap)	3.2.1	IEEE 802.11 wireless hub, a special kind of station (STA) operating as an access point.
basic service set (bss)	3.2.2	Coverage area served by one access point (AP).
cryptographic algorithm	3.2.3	A cryptographic algorithm is the means by which data are altered and disguised in encryption.
cyber environment	3.2.4	This includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks
cybersecurity	3.2.5	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity (which may include authenticity and non-repudiation) and, Confidentiality.
distributed system	3.2.6	A non-standardized medium for interconnecting BSSs within an ESS
extensible authentication protocol	3.2.7	This PPP extension providing support for additional authentication methods is part of the [b-IEEE 802.1X] specification.
extended service set	3.2.8	A single wireless LAN with BSSs within a single IP subnet.
firewall	3.2.9	A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.
foreign agent	3.2.10	The visited/host network's router that services the mobile node while it is visiting the host network. This foreign agent handles the tunnelling and delivery between the mobile node and others, and between the mobile's home network and the host network.
honeyspot	3.2.11	A software program that emulates a network so as to attract (and maybe confuse) intruders and track their actions. The output of these systems can be used to infer the intruder's intentions and evidence gathering.
home agent	3.2.12	A router that services the mobile node while it is visiting other networks,

		maintaining current location information on that mobile node.
hot spots	3.2.13	Public places that host mobile IEEE 802.11 users to connect to the Internet.
IP mobility	3.2.14	A mechanism which enables more transparent connectivity for mobile nodes that "visit" different IP sub-networks while travelling. This is a mechanism for mobile management for mobile nodes on both wired networks and wireless networks

Document:	**ITU-T X.800**	
access control	3.3.1	The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner
access control list	3.3.2	A list of entities, together with their access rights, which are authorized to have access to a resource
accountability	3.3.3	The property that ensures that the actions of an entity may be traced uniquely to the entity.
active threat	3.3.4	The threat of a deliberate unauthorized change to the state of the system.
authentication	3.3.7	Data origin authentication, and peer entity authentication.
authentication information	3.3.8	Information used to establish the validity of a claimed identity.
authentication exchange	3.3.9	A mechanism intended to ensure the identity of an entity by means of information exchange.
authorization	3.3.10	The granting of rights, which includes the granting of access based on access rights.
availability	3.3.11	The property of being accessible and useable upon demand by an authorized entity.
capability	3.3.12	A token used as an identifier for a resource such that possession of the token confers access rights for the resource.
channel	3.3.13	An information transfer path.
ciphertext	3.3.14	Data produced through the use of encipherment. The semantic content of the resulting data is not available. Note – Ciphertext may itself be input to encipherment, such that super-enciphered output is produced.
cleartext	3.3.15	Intelligible data, the semantic content of which is available.
confidentiality	3.3.16	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
credentials	3.3.17	Data that is transferred to establish the claimed identity of an entity.
cryptanalysis	3.3.18	The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext.
cryptographic checkvalue	3.3.19	Information which is derived by performing a cryptographic transformation (see cryptography) on the data unit.
cryptography	3.3.20	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.
data integrity	3.3.21	The property that data has not been altered or destroyed in an unauthorized manner.
data origin authentication	3.3.22	The corroboration that the source of data received is as claimed.
decipherment	3.3.23	The reversal of a corresponding reversible encipherment.
decryption	3.3.24	As decipherment.

denial of service	3.3.25	The prevention of authorized access to resources or the delaying of time-critical operations.
digital signature	3.3.26	Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient
encipherment	3.3.27	The cryptographic transformation of data (see cryptography) to produce ciphertext
end-to-end encipherment	3.3.29	Encipherment of data within or at the source end system, with the corresponding decipherment occurring only within or at the destination end system.
identity-based security policy	3.3.31	A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.
key	3.3.32	A sequence of symbols that controls the operations of encipherment and decipherment.
key management	3.3.33	The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.
link-by-link encipherment	3.3.34	The individual application of encipherment to data on each link of a communications system.
manipulation detection	3.3.35	A mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally).
masquerade	3.3.36	The pretence by an entity to be a different entity.
notarization	3.3.37	The registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery.
passive threat	3.3.38	The threat of unauthorized disclosure of information without changing the state of the system.
password	3.3.39	Confidential authentication information, usually composed of a string of characters.
peer-entity authentication	3.3.40	The corroboration that a peer entity in an association is the one claimed.
physical security	3.3.41	The measures used to provide physical protection of resources against deliberate and accidental threats.
privacy	3.3.43	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. Note – Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.
repudiation	3.3.44	Denial by one of the entities involved in a communication of having participated in all or part of the communication.
routing control	3.3.45	The application of rules during the process of routing so as to chose or avoid specific networks, links or relays.
rule-based security policy	3.3.46	A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users.

security audit	3.3.47	An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures
security audit trail	3.3.48	Data collected and potentially used to facilitate a security audit.
security label	3.3.49	The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
security policy	3.3.50	The set of criteria for the provision of security services
security service	3.3.51	A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
selective field protection	3.3.52	The protection of specific fields within a message which is to be transmitted.
sensitivity	3.3.53	The characteristic of a resource which implies its value or importance, and may include its vulnerability.
threat	3.3.55	A potential violation of security.
traffic analysis	3.3.56	The inference of information from observation of traffic flows (presence, absence, amount, direction and frequency).
traffic flow confidentiality	3.3.57	A confidentiality service to protect against traffic analysis.
traffic padding	3.3.58	The generation of spurious instances of communication, spurious data units and/or spurious data within data units.
trusted functionality	3.3.59	Functionality perceived to be correct with respect to some criteria, e.g. as established by a security policy.

Document:	**ITU-T X.805**	
Security dimension		A set of security measures designed to address a particular aspect of the network security. These dimensions are not limited to the network, but extend to applications and end user information as well. In addition, the security dimensions apply to service providers or enterprises offering security services to their customers.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-01-15-934-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-155-7
DOI: 10.2824/4069